

# CYBER SECURITY FOR STARTUPS

*A practical approach to start your security journey*



**Rohit Srivastwa**  
**Aalok Karnik**

This e-book is dedicated to all the startup founders who have the courage and vision to pursue their dreams, despite the challenges they may face along the way.

May this e-book empower you with the knowledge and skills needed to protect your business and its sensitive data from cyber threats, allowing you to focus on what you do best - innovating and growing your startup.

## Table of Contents

Chapter 1: Why Information Security Matters for Startups.....	4
1.1 Vulnerability.....	4
1.2 Consequences .....	4
1.3 Evolution of Startups .....	5
1.4 Learning from this e-Book .....	6
Chapter 2: Regulatory Requirements for Startups .....	7
2.1 Privacy Laws .....	7
2.2 Data Protection Laws.....	7
2.3 Cybersecurity Laws.....	7
2.4 Indian Laws .....	7
2.5 CERT-In Directives .....	8
Chapter 3: Information Security Fundamentals .....	9
3.1 Confidentiality, Integrity, and Availability (CIA).....	9
3.2 Threat Modelling.....	9
3.3 Risk Management.....	10
3.4 Continuous Improvement Cycle.....	10
Chapter 4: Information Security for Early-Stage Startups.....	11
4.1 Foundational Security Practices .....	11
4.2 Information Security Policies and Procedures .....	12
4.3 Third-Party Risk Management .....	12
Chapter 5: Information Security for Growth-Stage Startups.....	13
5.1 Access Control.....	13
5.2 Vendor & 3 <sup>rd</sup> Party Management .....	13
5.3 Vulnerability Assessment and Penetration Testing.....	14
5.4 Employee Education and Training.....	14
5.5 Building a security team .....	14
Chapter 6: Information Security for Established Startups .....	15
6.1 Information Security Program .....	15
6.2 Periodic Penetration Testing.....	15
6.2.1 Application Penetration Testing.....	16
6.2.2 API Penetration Testing .....	16
6.2.3 Network Penetration Testing .....	16
6.3 Cybersecurity Team.....	16
6.4 Logging and Monitoring.....	16
6.5 Cyber Insurance .....	16
6.6 Think beyond Anti-Virus and Firewall .....	17
Chapter 7: Information Security for Cloud-Based Startups.....	18

7.1 Cloud Provider Selection .....	19
7.2 Cloud Security Best Practices .....	19
7.3 Monitoring .....	19
Chapter 8: Information Security for Remote Workforces .....	20
8.1 Secure Remote Access .....	20
8.2 Secure Remote Support .....	20
8.3 Ongoing Awareness and Training .....	20
Chapter 9: Incident Response Planning .....	21
9.1 Incident Response Team .....	21
9.2 Incident Response Plan .....	21
9.3 Incident Response Drills .....	22
9.4 Learnings from Incidents .....	22
Chapter 10: Log Management .....	23
10.1 Logging .....	23
10.2 Alerting .....	23
10.3 Monitoring .....	23
10.4 Reporting .....	23
10.5 Security Information Event Management (SIEM) .....	24
10.6 Adhering to CERT-In Directives (2022) .....	24
10.7 Outsource security monitoring (If needed) .....	24
10.8 Logs and attack scenario .....	25
Chapter 11: Data Lifecycle Management .....	26
11.1 Data Collection .....	26
11.2 Data Classification .....	26
11.3 Data Security .....	27
11.4 Data Disposal .....	27
11.5 Code = Data .....	27
Conclusion .....	28

## Chapter 1: Why Information Security Matters for Startups

As an entrepreneur, you are aware that information security is a challenge arising from building and growing a new business. Unfortunately, information security is often deprioritized over say product development or marketing.

Implementing effective information security measures from the outset is crucial for startups to protect their intellectual property, customer data, and ward off potential litigation.

Two types of organizations: those that **have been** breached and those that **will be** breached.

### 1.1 Vulnerability

Startups are often particularly vulnerable due to their limited resources and the fast-paced, agile nature of their operations. While larger companies may have dedicated security teams and significant budgets for cybersecurity, startups may not have the same level of resources available to them.

This can make you an attractive target for cybercriminals who exploit vulnerabilities and steal valuable data.

### 1.2 Consequences

The consequences of a security breach for a startup can be devastating.



**Data theft**



**Loss of customer trust**



**Legal and regulatory penalties**

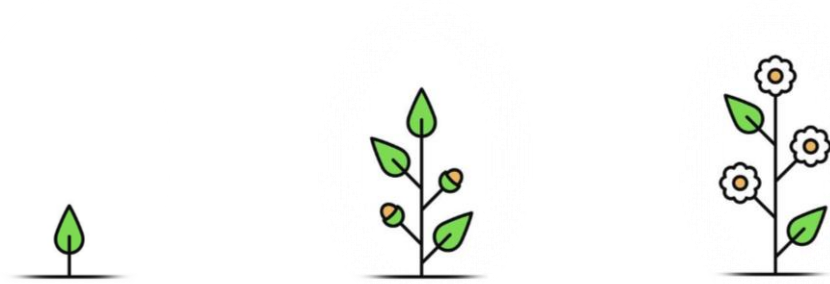


**Bankruptcy in extreme cases**

Given the high stakes involved, startups must take information security seriously and implement appropriate measures and practices to protect their intellectual property.

### 1.3 Evolution of Startups

As startups grow and mature, their information security needs evolve along with them. In the early stages, startups are focused primarily on product building and acquiring customer acquisition, with little attention paid to information security. But with time the strength of an organization increases and so does the importance to protect its intellectual property and related processes.



	Early	Growth	Established
<b>Status</b>	Just off ground. Focus on product/service development	Rapid scaling of operations	Significant success with product/service. Focus on acquisitions, mergers
<b>Team Size</b>	Small	Medium	Large
<b>Funding</b>	Limited/minimal. High dependency on external funding	Limited revenue streams. Increased funding due to scaling	Multiple revenue streams. Limited external funding
<b>Presence</b>	Negligible	Local	Global
<b>Customer Base</b>	Limited/minimal	Broad	Large
<b>Security Program</b>	Basic	Adopt industry best practices	Adherence to global standards
<b>Security Cost</b>	Limited/minimal	Elevated	High
<b>Security Deployment</b>	AV, IAM, firewall, encryption, cloud usage, access control, MFA	<b>[Early]</b> + asset management, logging, alerting, basic DLP, training, specialist hiring	<b>[Growth]</b> + SIEM, DLP, SWG, CASB, PAM, audits, certifications, VAPT, SOC

**Note:** 'Security Deployment' parameter will vary per organization's needs.

Company growth attracts more customers and partners as product/service gains foothold in the market, therefore risks associated with a security breach become more significant.

## 1.4 Learning from this e-Book

In this e-Book, we will explore the various stages of a startup's development and provide guidance on how to focus on information security throughout each stage, from ideation and planning to maturity and stability.

By implementing industry standard security controls, measures and practices, startups can:



Protect intellectual property and operations.



Gain a competitive edge by demonstrating security commitment to stakeholders.



Achieve audit compliance by adopting industry standard best practices.



Reduce the risk of breaches and other security incidents.



Build a foundation for long-term success.

In the following chapters, your startup can implement specific recommendations and actionable steps to strengthen your information security posture and protect yourself against cyber threats.

## Chapter 2: Regulatory Requirements for Startups

As a startup, it is important to understand regulatory requirements applicable to your business. These regulations vary depending on the industry, location, and business size. In this chapter, we discuss common global regulatory requirements that startups should be aware of and steps to achieve compliance.

### 2.1 Privacy Laws

In the United States, the California Consumer Privacy Act (CCPA) is the primary privacy related law.

### 2.2 Data Protection Laws

In the European Union: General Data Protection Regulation (GDPR) is mandated for data protection.


In the United States: Health Insurance Portability and Accountability Act (HIPAA) is mandated for healthcare data.

### 2.3 Cybersecurity Laws

In the United States: Cybersecurity Act of 2015 is mandated for cybersecurity of networks and systems.

### 2.4 Indian Laws

In India, information security is governed by various laws and regulations that establish requirements for companies operating in India to protect sensitive, personal, and financial data of their customers and employees.

	<b>IT Act of 2000 (2008 amendment)</b> The Act mandates that companies implement reasonable security practices and procedures to protect electronic data and prevent unauthorized access, use, disclosure, or destruction of data.
	<b>IT Rules (2011)</b> Mandate companies take reasonable steps to protect sensitive personal information and implement appropriate security measures.
	<b>Proposed Digital India Act (2023)</b> Sets out comprehensive requirements for the collection, processing, and storage of personal data. Includes requirement to obtain explicit consent from individuals for collection & use of their data.
	<b>RBI Guidelines</b> Banks and other financial institutions are subjected to stringent information security requirements for secure online banking and transaction processing.

Companies operating in India should be aware of these laws and regulations and take appropriate steps to meet compliance requirements and avoid potential legal and financial penalties.



## 2.5 CERT-In Directives

In 2022, CERT-India released directives related to reporting cyber security incidents within 6 hours of knowing about an incident. This needs deployments of platforms that detect intrusion attempts via automation, rules, extended logging mechanisms, and other means.

Reporting cybercrimes / intrusions outside the required timeframe could attract penalty and fines imposed on the organization by CERT-In.

Startups need to consider that cybercrimes can be reported if and only if there is a robust detection mechanism in place. This is not possible manually; hence automation should be an integral part of intrusion detection within your environment.

To assist companies in demystifying the complexities involved with deployment of these directives we have written an easy-to-understand document:

[\[https://www.rohit11.com/2022/06/12/demystifying-cert-in-directives-dated-28th-april-2022/\]](https://www.rohit11.com/2022/06/12/demystifying-cert-in-directives-dated-28th-april-2022/)

Official CERT-In documents linked here for your reference:

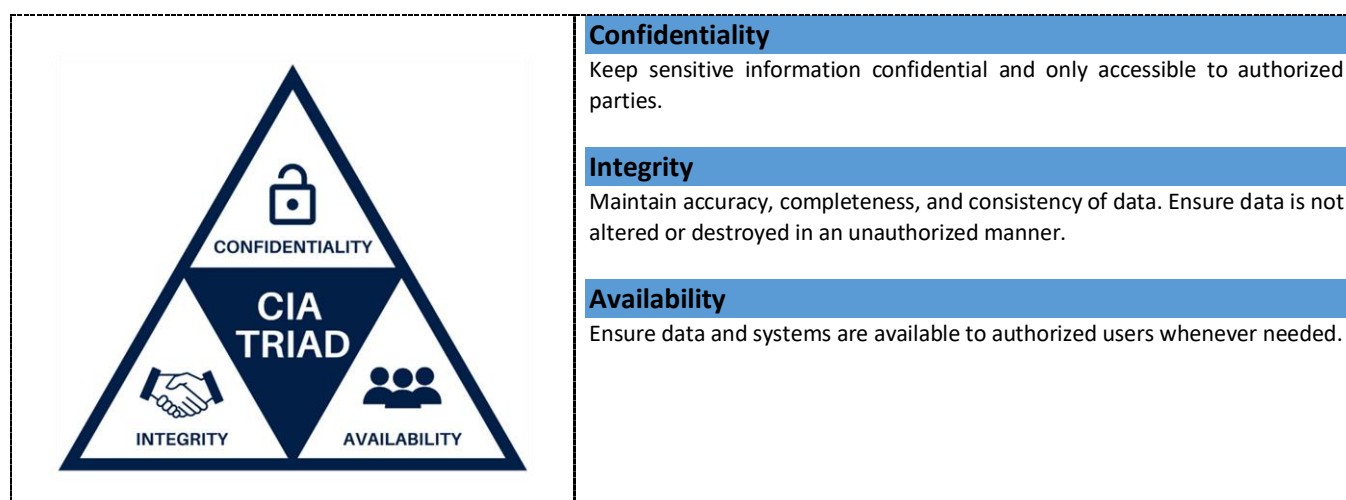
- [CERT-In Directions 70B 28.04.2022.pdf](#)
- [FAQs on CyberSecurityDirections May2022.pdf \(cert-in.org.in\)](#)
- [CERT-In directions extension MSMEs and validation 27.06.2022.pdf](#)

## Chapter 3: Information Security Fundamentals

Before we dive into the specific information security practices for startups, it's essential to understand the fundamental principles that underpin effective security measures. Here are some of the key concepts to keep in mind:

### 3.1 Confidentiality, Integrity, and Availability (CIA)

These are the three principles that guide general information security practices.

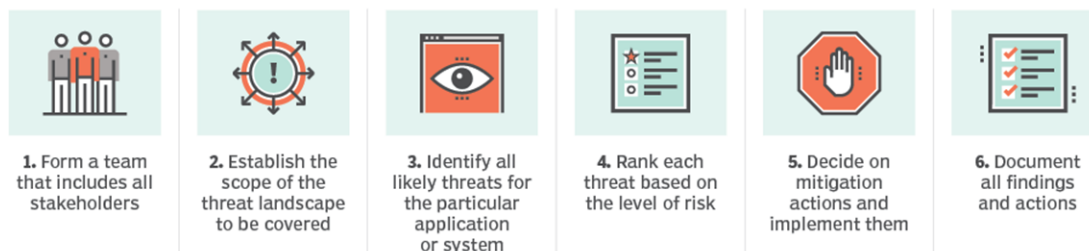


### 3.2 Threat Modelling

It is a process of identifying potential threats and vulnerabilities to your organization's systems and data. By understanding the various types of threats that you may face, you can effectively prioritize and implement security measures to protect your organization.

There are various threat modelling paradigms (PASTA, STRIDE, MITRE etc) and the involved steps may vary but the overall idea is the same.

## 6 steps in the threat modeling process



[Read More: <https://www.techtarget.com/searchsecurity/definition/threat-modeling>]

### 3.3 Risk Management

Risk management is a process of identifying and addressing potential risks to your organization. It involves assessing the likelihood and potential impact of each risk and then implementing measures to mitigate or eliminate those risks.

## The five-step risk management process

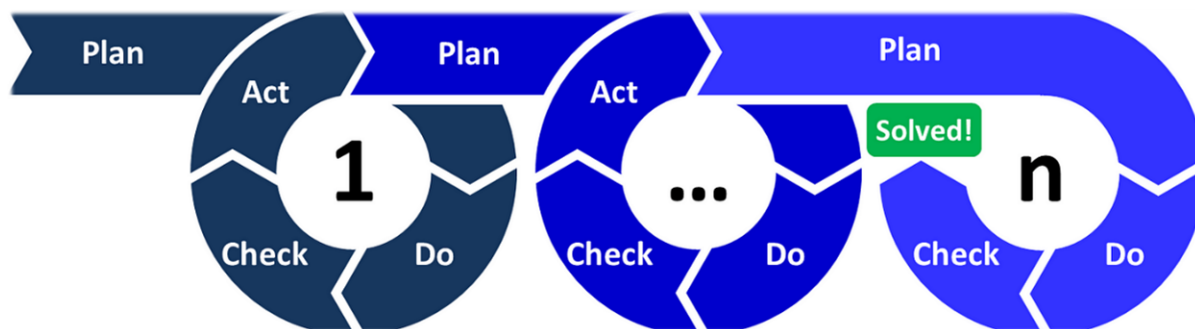


[Read more: <https://www.techtarget.com/searchsecurity/definition/What-is-risk-management-and-why-is-it-important>]

### 3.4 Continuous Improvement Cycle

Throughout your evolution protect your data and assets.

- Remain vigilant and proactive in your approach to information security.
- Continually assess your risks.
- Implementing appropriate measures until resolution.



[Read More: <https://medium.com/@amine.rouh/continuous-improvement-with-pdca-357ae742bc49>]

## Chapter 4: Information Security for Early-Stage Startups



Early-stage startups face unique challenges when it comes to information security. Due to limited resources and product/service centric focus, information security could take a backseat. However, implementing basic security measures from the start will help protect the intellectual property critical to a startup's success.

Do not shy away from integrating industry standard platforms/tool within your environment as they allow increased productivity while meeting security requirements.

### 4.1 Foundational Security Practices

Early-stage startups should prioritize implementing foundational security practices, including:

<b>Secure Productivity</b>	Deploy industry standard secure platforms such as Google Workspace/Microsoft 365/Zoho etc. as they provide additional features (e.g., user management, access control, encryption etc.)
<b>Secure Emailing</b>	Email access can be provided as needed to users. Email can be monitored for malware. Advanced monitoring can include data leakage protection.
<b>Secure File Sharing</b>	Leverage secure file sharing, storage solutions and processes for data access to authorized parties (investors, partners, users, etc). Achievable via productivity suites mentioned above.
<b>Asset Management</b>	Ensure all hardware inventory and software licenses are accurately tracked (even if in a spreadsheet) & periodically reviewed for completeness. You'll thank us later for this.
<b>Passwords</b>	Mandate and enforce complex passwords and push for regular password changes. Leverage password managers if possible. Remember Pa\$\$W0rd or Password@123 looks long and complex to satisfy most of the password policy requirements but it's not secure.
<b>Two-Factor Authentication</b>	Without fail implement two-factor authentication for all team members to prevent unauthorized access to company systems and data.
<b>Encryption</b>	Encryption is a powerful tool for protecting information in transit and at rest. Startups should consider using encryption for all communication and file transfers. Note that password protecting a file does not count as encryption. Also adding SSL/TLS on website is not the end of encryption, there is more to it.

## 4.2 Information Security Policies and Procedures



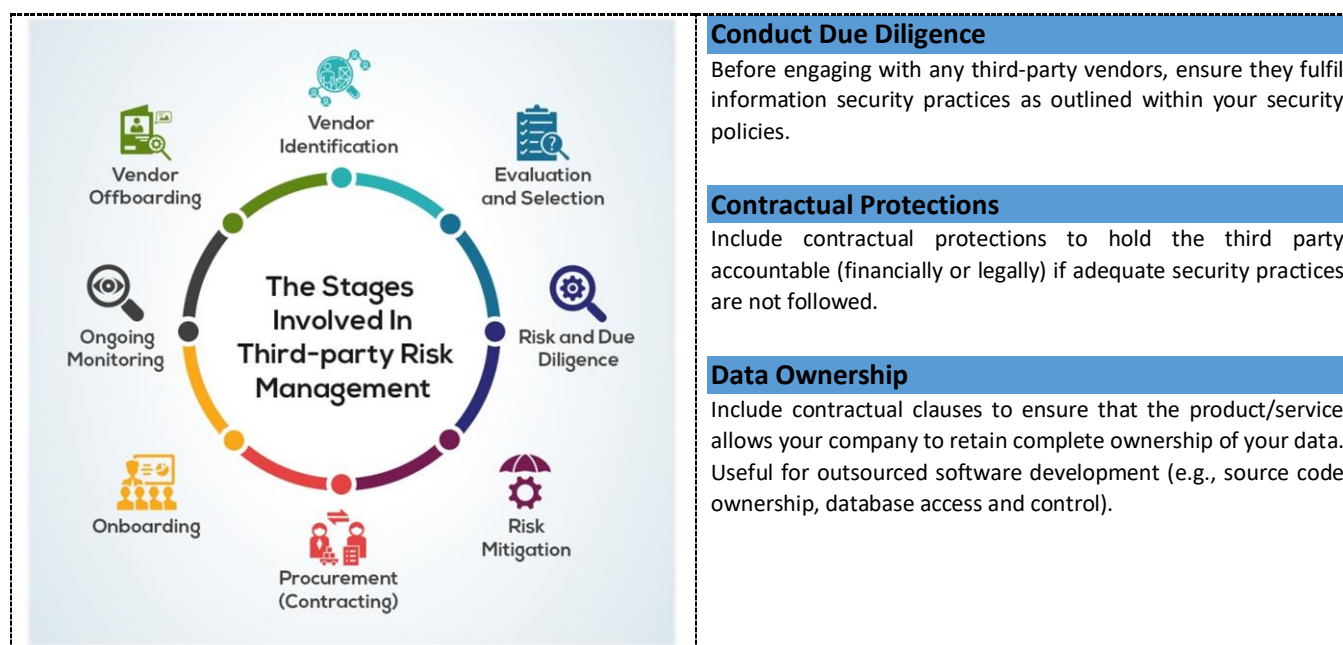
Implementing information security policies and procedures is another critical step for early-stage startups. It may sound mundane, but it is critical to start early since all actions, security controls etc. will be implemented based on these policies. All policies and SOPs will (& should) be updated over time as team's maturity increases.

<b>Information Security Policy</b>	Draft an overarching information security policy (however basic in content). Implement within the organization and fine-tune as needed. Include enhancements as part of a continuous improvement process.
<b>Acceptable Use of Company Assets</b>	Establish guidelines and rules for how team members should use company assets, systems, and data. Include guidelines to dictate how user devices can access, use, store, manage, share, and destroy company systems and data.
<b>Backup Planning</b>	Develop a robust backup process as it will be your saviour in case of any incident. Outlines the steps that team members will perform for accurate backup and data storage. This is crucial for business continuity and disaster recovery. Remember a good backup plan includes periodic restoration testing as well.
<b>Standard Operating Procedures (SOP)</b>	Develop SOPs for various tasks that will allow authorized personnel to complete tasks during normal operations or during an incident (e.g.: primary personnel is unavailable).

## 4.3 Third-Party Risk Management

Early-stage startups often rely on third-party vendors for various services, such as development, web hosting or payment processing, etc. However, these vendors can also pose a security and compliance risk if proper security practices are not adhered to.

Remember this process is complex hence it is advisable to start small and early.



By implementing these foundational security practices, early-stage startups can reduce their risk of security incidents and start building a solid foundation for information security.



## Chapter 5: Information Security for Growth-Stage Startups

Growth-stage startups have slightly elevated levels of information security needs given they may have a larger team, increased funding, and a broader customer base, which translates to implementing advanced security measures and processes to protect their intellectual property, data, and operations.

### 5.1 Access Control

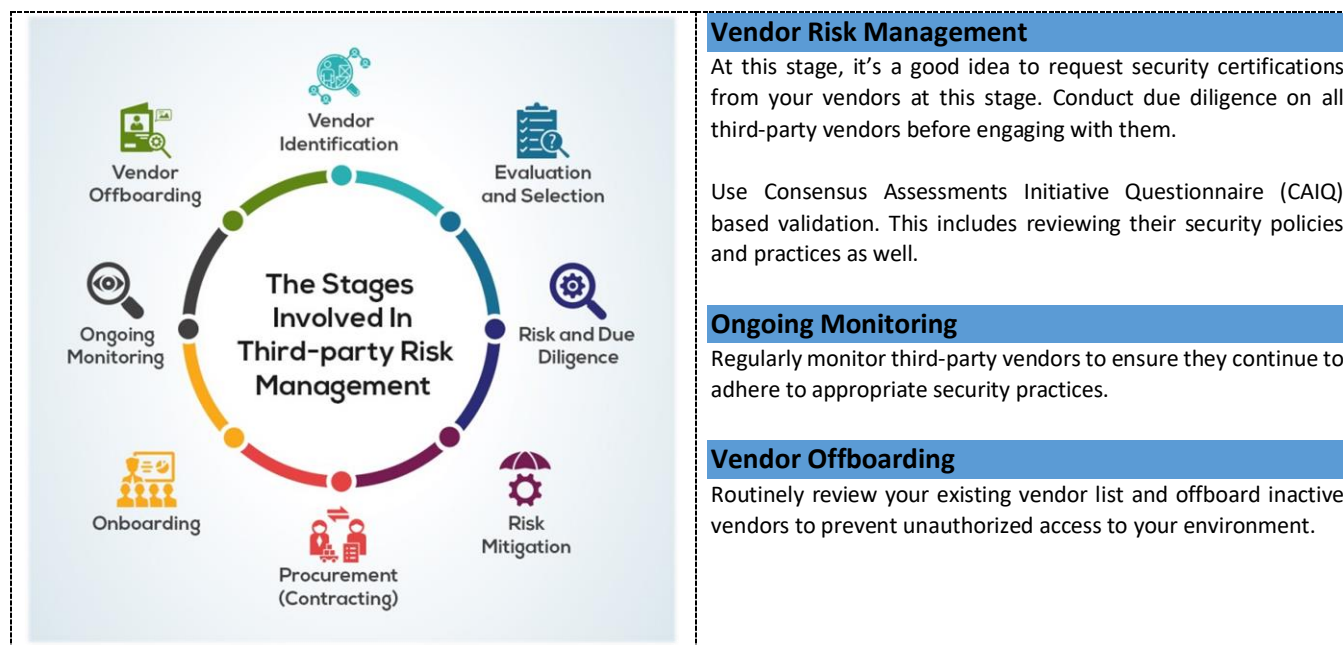
At this stage ensure only authorized team members have access to information systems and data on an as-needed basis. Implementing access control measures protect against security breaches.

Key access control measures that growth-stage startups should consider include:

<b>Segregation of Duties</b>	In early startups, many a times literally everyone is an administrator and has elevated privileges. Start segregation of duties early on to save future pains.
<b>Role-Based Access Control</b>	Assign roles and permissions to each team member based on their job responsibilities.
<b>Monitoring and Auditing</b>	Implement monitoring and auditing mechanisms to track how and by whom sensitive information and systems are being accessed.

### 5.2 Vendor & 3<sup>rd</sup> Party Management

Remember the tedious process of vendor management? Few more steps need to be implemented during the growth stages. Now it's likely that you will work with more vendors and third-party service providers. It's essential to ensure that all third-party vendors adhere to proper security practices.






### 5.3 Vulnerability Assessment and Penetration Testing

As your product reaches a go-live stage, do conduct a vulnerability assessment and penetration testing (VAPT). These tests can identify potentially exploitable weaknesses that could be used by attackers.

VAPT allows your organization to ship a secure product (USP) reducing the potential for a security incident.

### 5.4 Employee Education and Training

	<p><b>Security is everyone's responsibility.</b></p> <p>It's critical that ALL team members understand their roles and responsibilities when dealing with information security.</p> <p>Routine education and training programs on security best practices will create awareness and help reduce security incidents caused by human error.</p>
--	---

Growth-stage startups should consider implementing:

Security Training	Conduct routine security training for all team members to educate them on industry best practices and updated policies.
Phishing Simulations	Conduct phishing simulations to test team members ability to identify and report phishing attempts.
Incident Response Drills	Conduct routine incident response drills to ensure that all team members understand their roles and responsibilities during a security incident.

### 5.5 Building a security team

While IT support personnel is commonly assigned information security responsibilities, relying solely on them may lead to negative consequences. This is because IT staff may lack the necessary expertise to manage an enterprise-level information security program. It is advisable to hire specialized staff and establish an in-house security team to achieve segregation of duties between security and IT.

Another viable option is to engage an external consultant to design a security program and aid the IT team in deploying security controls, which can significantly enhance your security profile. The external consultant can also assist in building the security team as required.

By implementing these intermediate level security measures and processes, growth-stage startups can better protect their data and operations and prevent security incidents that could undermine their growth and success.



## Chapter 6: Information Security for Established Startups

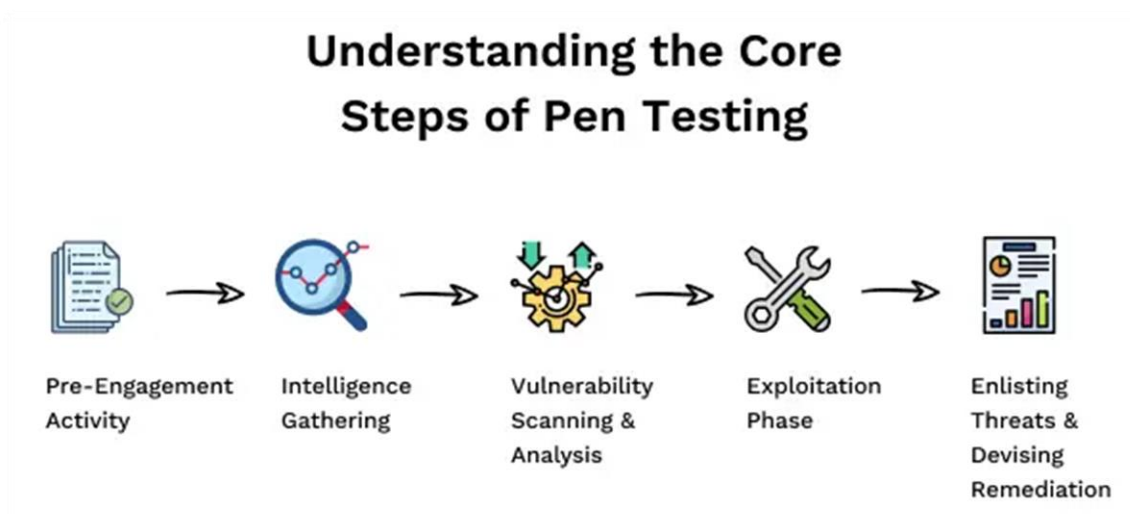
As a startup reaches the established stage, it likely has a large customer base, complex business processes, and a significant amount of sensitive data to protect. At this stage, implementing a comprehensive information security program is critical for protecting the organization's customer data, intellectual property, and reputation.

### 6.1 Information Security Program

Established startups should implement a comprehensive information security program. This program should include policies and procedures for:

<b>Incident Response Planning</b>	Develop a detailed incident response plan that outlines the organizational response plan to security incidents.
<b>Risk Management</b>	Conduct regular risk assessments to identify potential risks and vulnerabilities to the organization's systems and data.
<b>Compliance</b>	Ensure that the organization is compliant with all relevant security and privacy regulations, such as GDPR or HIPAA.
<b>Third-Party Risk Management</b>	Establish rigorous vendor management processes to ensure that third-party vendors adhere to appropriate security practices.
<b>Change Management</b>	<p>Develop a clear and comprehensive plan for managing changes to your business processes, communication, and culture, and ensure that all stakeholders are engaged and informed throughout the implementation process.</p> <p>This helps immensely during disaster recovery (rollback), incident management (evidence), and audits (accountability) purposes.</p>

### 6.2 Periodic Penetration Testing



[Read More: <https://securetriad.io/web-applications-penetration-testing/> ]





### 6.2.1 Application Penetration Testing

Conduct routine penetration testing for your application development environment to reduce the chances of shipping a product with security issues and allows an organization to gain a competitive advantage. An established product/service is a prime target for attackers.

If your development environment has a strong codebase supported by robust processes, then consider adopting Responsible Vulnerability Disclosure Program (RVDP AKA Bug Bounty) as well. For outsourced software development, you should request the agency to provide you with a copy of their penetration testing report.

### 6.2.2 API Penetration Testing

If your startup deals with APIs, let me tell you that investing in API security and penetration testing is not just a good practice but a necessity in today's digital landscape! APIs are the backbone of your business, and any breach or vulnerability in them could put your entire business at risk.

Don't limit yourself to simple application penetration testing only.

### 6.2.3 Network Penetration Testing

Network penetration testing is also performed to ascertain exploitable gaps that will be used by attackers to infiltrate the network and gain access to high value assets. Do that occasionally, especially after bigger changes in the network structure.

## 6.3 Cybersecurity Team

At this point, your organization should have a mature security team led by a Chief Information Security Officer (CISO). This team bears the responsibility of enforcing your security program, ensuring continual improvement, conducting security monitoring, managing incidents, planning, budgeting, liaising with authorities, maintaining compliance, and overseeing vendor management.

Moreover, the security team plays a pivotal role in creating a culture of cybersecurity within the organization by promoting security awareness and knowledge among all team members and ensuring the seamless integration of security measures across all operations.

To enhance the effectiveness of your security team, you may consider bringing in a virtual CISO who can support your in-house team and oversee your security program.

## 6.4 Logging and Monitoring

By implementing logging and monitoring, you can identify and troubleshoot issues quickly, reducing downtime and improving customer satisfaction. You can also improve security by detecting and responding to threats in real-time. Proper logging and religious monitoring can help you meet compliance requirements and provide transparency.

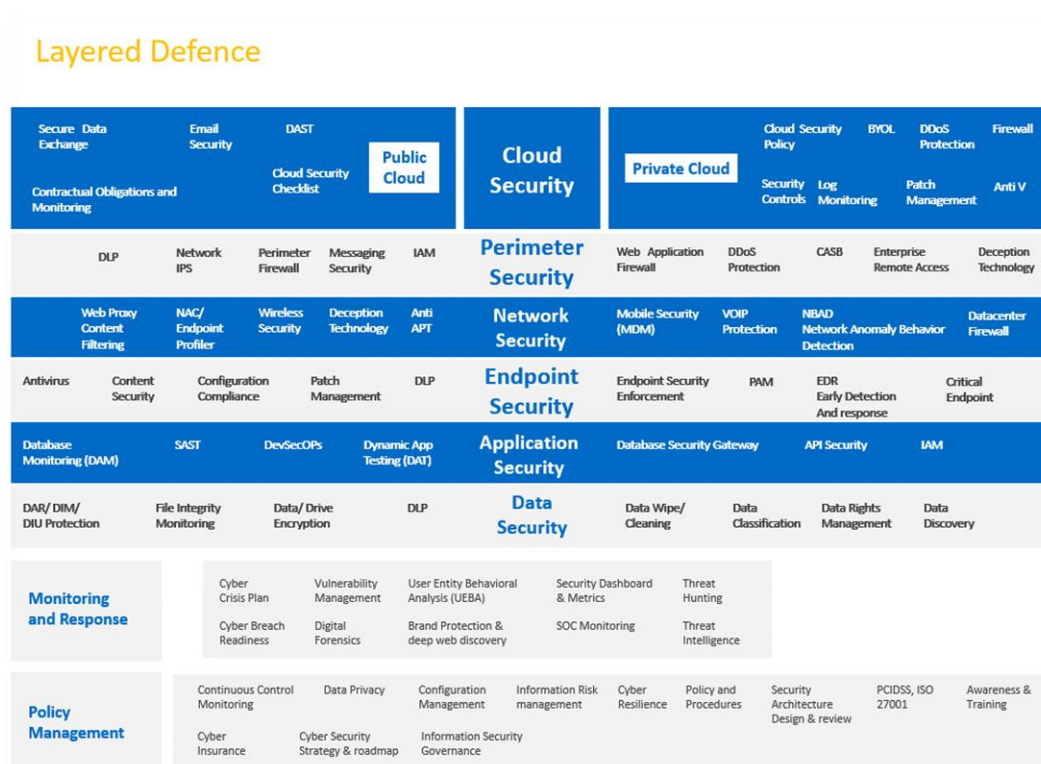
This is so critical that it mandates its own chapter. Refer to chapter 10 for more information.

## 6.5 Cyber Insurance

Established startups should also consider purchasing cyber insurance to protect against potential financial losses resulting from any security incident. Cyber insurance policies can provide coverage for costs related to data breach response, legal fees, and settlement payments.

## 6.6 Think beyond Anti-Virus and Firewall

As a company grows your erstwhile investments in simple antivirus, firewall etc may not suffice. It's time to rethink the complete security stack which will be done by your CISO and/or vCISO. Now you must have a layered security approach to fortify your infrastructure and protect your crown jewels.



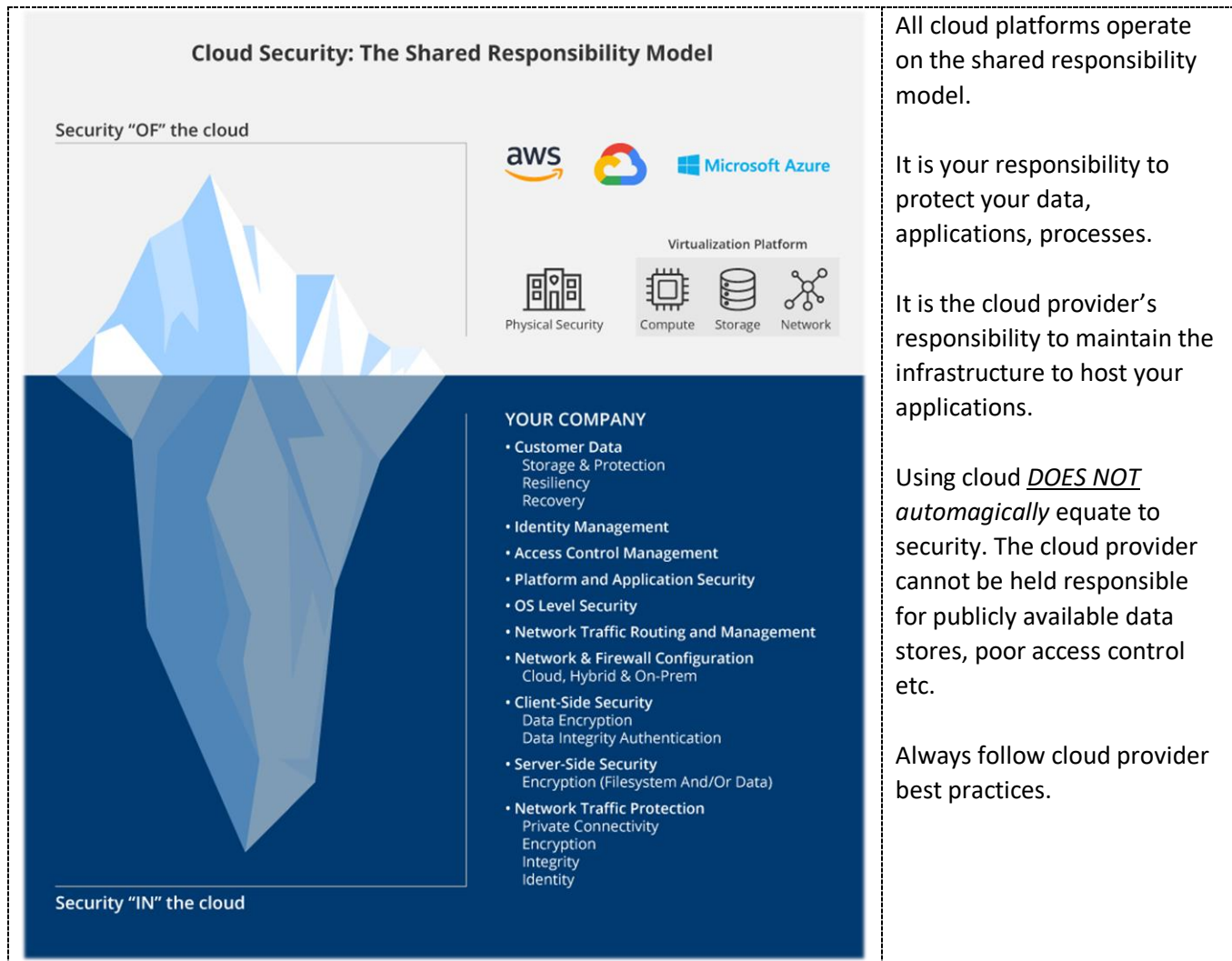
Here are few scoops from the alphabet soup of security technologies.

<b>EDR</b>	<b>Endpoint Detection and Response</b>	Go beyond antivirus, this is needed for new age malware protection including ransomware. It uses the power of CTI on AV
<b>CASB</b>	<b>Cloud Access Security Broker</b>	Provide security enforcement and visibility for organizations using cloud-based services. Using cloud, must consider CASB
<b>SWG</b>	<b>Secure Web Gateway</b>	Protect users from web-based threats and control access to potentially harmful websites. Take firewall rules along with user wherever they are
<b>ZTNA</b>	<b>Zero Trust Network Access</b>	Provide secure remote access to applications and resources while assuming no inherent trust for devices, networks, or users.
<b>PAM</b>	<b>Privileged Access and Monitoring</b>	Secure, monitor, and manage access to privileged accounts and critical systems within an organization. Keep a track on system administrators' activities on the servers
<b>DLP</b>	<b>Data Leakage Prevention</b>	Protect sensitive data by identifying, monitoring, and preventing data breaches, leakage, or theft both at rest and in motion.
<b>UEM</b>	<b>Unified Endpoint Management</b>	Provide a centralized platform for managing and securing endpoints, including mobile devices, laptops, and desktops, across an organization.
<b>NAC</b>	<b>Network Access Control</b>	Control and secure access to a network by ensuring that only authorized and compliant devices and users can connect to it.
<b>CTI</b>	<b>Cyber Threat Intelligence</b>	Provide organizations with actionable intelligence on current and emerging threats to proactively defend against cyber-attacks.
<b>FDE</b>	<b>Full Disk Encryption</b>	Encrypt all data on a disk or device to prevent unauthorized access in case of theft or loss or laptop and/or hard drives.
<b>IAM</b>	<b>Identity and Access Management</b>	Ensure that only authorized individuals have access to specific resources within an organization's IT infrastructure.

## Chapter 7: Information Security for Cloud-Based Startups

Many startups today rely on cloud-based solutions to run operations, store, and manage their data. Cloud environments provide many benefits and come with unique security challenges. Leverage pre-built security platforms/tools part of the selected cloud plan and fine-tune them to protect data from potential threats.

This applies to IaaS, PaaS, SaaS and all other as-a-Service offerings.



All cloud platforms operate on the shared responsibility model.

It is your responsibility to protect your data, applications, processes.

It is the cloud provider's responsibility to maintain the infrastructure to host your applications.

Using cloud DOES NOT automatically equate to security. The cloud provider cannot be held responsible for publicly available data stores, poor access control etc.

Always follow cloud provider best practices.

[Read More: <https://www.binadox.com/blog/shared-responsibility-model-for-cloud-security/>]

## 7.1 Cloud Provider Selection

Startups must ensure their cloud service provider adheres to industry security practices. You should be able to view their certifications posted online. This also applies to SaaS platforms.

Although all the cloud providers simplify the signup process by just swiping a credit card, it is highly recommended to proceed via a local reseller. They can help in negotiations and would be your conduit for support requirements. These resellers are well equipped to handle most issues and know the best support escalation options available for you.

## 7.2 Cloud Security Best Practices

Every cloud provider has a set of recommendations as part of their best practices for information security. Startups should implement those best practices to ensure the data security.

<b>Strong Access Control</b>	Use strong access control mechanisms, including multi-factor authentication, to ensure that only authorized users can access the cloud resources.
<b>Data Encryption</b>	Encrypt all data stored on the cloud as well as in transit to protect against unauthorized access.
<b>Regular Backups</b>	Regularly backup all data stored on the cloud to ensure an up-to-date copy of the data. Leverage cloud backup solutions for the same
<b>Network Segmentation</b>	Segment the cloud network such that one compromised node cannot lead to a complete network breach.

Additionally, cloud providers publish security recommendations and/or security scorecard, following the same will boost your security posture.

## 7.3 Monitoring

Like an on-premises environment, it is critical to monitor your cloud platforms, resources, and services for potential security incidents. Keep an eye out for security incident news about your cloud provider. If you are aware of any cloud provider related security incident, you can take timely remedial action to protect your cloud resources from data loss/theft.

## Chapter 8: Information Security for Remote Workforces

As remote work becomes more common, startups must adopt additional information security practices protecting their data and systems from security threats arising from remote work. With team members working across geographies and devices, it's crucial to implement security measures that ensure the confidentiality, integrity, and availability of sensitive information.

### 8.1 Secure Remote Access

Secure remote access is critical for protecting company data from unauthorized access. Remote access should be restricted to authorized users and devices, and mandate strong authentication, such as multi-factor authentication. Startups can implement secure remote access by:

<b>Virtual Private Networks (VPNs)</b>	Creates a secure connection between a remote user's device and the company network.
<b>Virtual Desktop Infrastructure (VDI)</b>	Provide remote users with a virtual desktop hosted on the company network.
<b>Zero Trust Network Access (ZTNA)</b>	Implementing ZTNA will secure local and remote access to company infrastructure from all devices (including remote workstation).

### 8.2 Secure Remote Support

Users can face access issues, connectivity issues and a host of other problems. These scenarios need intervention from IT support staff. DO NOT blindly permit Remote Desktop Protocol (RDP), Secure Shell (SSH) via your firewall rules as this can open a pandora's box of issues. Leverage a secure remote desktop software platform that mandates MFA to resolve user issues.

### 8.3 Ongoing Awareness and Training

Continuous training and awareness program is important to maintain a healthy security posture. This will uplift security awareness culture within the organization and this effort should initiate early on.

Remote work can create additional security risks, especially with network security and home devices. To mitigate these risks, startups should provide ongoing awareness training to remote team members. Conduct regular security training to educate remote team members on security best practices not only for company provided devices but also for their personal home network and personal storage devices.

COVID has reinforced the importance of information security training for remote work scenarios. Startups must investigate and include remote work into their threat modelling scenarios.

## Chapter 9: Incident Response Planning

While startups can implement a variety of security measures to protect their data and systems, a security incident can still occur. As such, startups must develop and implement an incident response plan to ensure that they can respond quickly and efficiently in the event of a security incident.



[Read more: <https://www.webroot.com/blog/2018/07/25/6-steps-to-build-an-incident-response-plan/>]

[Read More: <https://www.devo.com/guide-to-the-future-soc/incident-response-process/>]

### 9.1 Incident Response Team

The first step in incident response planning is to identify and establish an incident response team. The team should include representatives from key departments, such as IT, legal, HR, management, and public relations. Training for the team is critical to be able to respond quickly to any security incident. Appropriate tools must be procured ahead of time to facilitate investigation and containment. Do not forget to train your team to use these tools.

### 9.2 Incident Response Plan

A comprehensive incident response plan should include the following key steps:

<b>Preparation</b>	Establish an incident response team, identify critical systems and data, and develop a communication plan.
<b>Detection and Analysis</b>	Monitor systems and networks for potential security incidents, investigate anomalies, and determine the nature and scope of the incident.
<b>Containment, Eradication, and Recovery</b>	Contain the incident, eradicate any malware or vulnerabilities, and recover any lost or damaged data or systems.
<b>Post-Incident Analysis</b>	Conduct a thorough analysis of the incident to identify any weaknesses or areas for improvement in the incident response plan.
<b>Communication</b>	Report the incident to relevant parties, such as regulatory authorities, clients, or shareholders.

Incident response plans will vary for networks, web applications, API's, user account breaches etc. All breaches cannot be prevented but having a plan to mitigate incident probability helps.

Identify the areas of exposure and develop a containment plan for them.

### 9.3 Incident Response Drills

*“Practice makes perfect”* and is true for an incident response plan to be effective. Startups should conduct regular incident response drills. These drills can help to identify any gaps in the plan and early steps can be taken to mitigate these gaps.

Practice allows the incident response team to respond quickly and efficiently during a security incident. Key considerations for incident response exercises include:

<b>Regularity</b>	Conduct incident response drills at least twice a year.
<b>Scenario Development</b>	Develop realistic scenarios that simulate potential security incidents.
<b>Team Involvement</b>	Involve the entire incident response team in the drills to ensure that everyone understands their roles and responsibilities.

Timely action is the foundation for an effective incident management program. It is critical that all entities know:

- activities to be performed and in which sequence.
- who is their predecessor and successor in the communication chain.
- formats of reports to be received and created at each level.
- process of follow-up until issue has been resolved (with verification).

### 9.4 Learnings from Incidents

Every incident presents an opportunity to learn and improve. Use them to boost your cyber security profile. Implement security measures to reduce or zero the probability of the same incident occurring again in the future.

Send out regular security bulletins to your workforce (e.g., phishing email alerts). This helps to build a security aware workforce that leads to a secure environment.

This could come at a cost and startups are well advised to factor security requirements in their operational expense (OpEx) budget.

Remember that incidents from neighbour organizations also serve as learning methods. Learn from their mistakes and improve your infrastructure and security measures.



## Chapter 10: Log Management

Effectiveness of an IT system is determined via its ability to detect and respond to potential issues, track system performance, and monitor overall health. All systems, platforms, applications, devices etc generate logs which can be analysed to identify issues, determine breaches, and sometimes serve as evidence during legal proceedings.

Collecting logs is trivial but managing them is another thing. However, the true value arises when actionable intelligence can be extracted from these logs over a timeframe. Extracting intelligence from logs manually is near impossible, will lead to mistakes, and miss potential intrusions.



[Read More: <https://lerablog.org/technology/software/top-6-advantages-of-log-management-software/>]

[Read More: <https://www.strongdm.com/what-is/log-management>]

Let's walk through the various stages from log collection to incident reporting.

### 10.1 Logging

Logging is the process of recording important events, actions, and errors that occur within a system or application. It's crucial for identifying and resolving issues, detecting, and preventing security breaches, and meeting regulatory compliance requirements. Effective logging requires careful consideration of what events should be logged, how much detail to capture, and how the logs will be stored and analysed. By maintaining detailed logs, businesses can improve system availability and protect their sensitive data.

### 10.2 Alerting

Alerting is the process of detecting and responding to potential issues in an IT system. It is used to identify potential problems before they become major issues. Alerts can be triggered by a variety of events, such as system outages, high resource utilization, or security breaches. Alerts can be sent to system administrators via email, text message, or other methods to action upon.

### 10.3 Monitoring

Monitoring is the process of ensuring that the system is running smoothly. It involves regularly checking system performance, resource utilization, and security. Monitoring can be done manually or automatically and can be used to detect potential issues before they become major problems.

### 10.4 Reporting

Reporting is the process of tracking system performance and usage. Reports can be used to identify trends, identify potential problems, and measure the effectiveness of system changes. Reports can be used to track system performance over time. It's a must to set a process of monitoring and reporting it to CERT-India in case of any attack identification.



## 10.5 Security Information Event Management (SIEM)

The industry standard solution for effective log management is to leverage Security Information Event Management (SIEM) platforms accessible via cloud solutions or an on-premise deployment. A SIEM is best used by a Security Operations Centre (SOC) that has dedicated personnel to collect & analyse logs followed by creating actionable alerts.



[Read More: <https://www.bitlyft.com/resources/siem-log-management-what-it-is-and-why-its-vital-for-cybersecurity>]

Leveraging a SIEM allows an organization to collate, correlate, and search logs across devices, applications etc (despite various formats) to present data in a dashboard so an analyst can identify issues within the environment. Resolving issues in a timely manner allows the organization to meet security and compliance requirements.

## 10.6 Adhering to CERT-In Directives (2022)

Remember the CERT-In directives we discussed in previous chapters; it directs that an organization should report identified security incidents to CERT-In within 6 hours. This is next to impossible without automation and usage of a SIEM platform. Failing to follow this directive, can lead to fines, potentially even jail time.

## 10.7 Outsource security monitoring (If needed)

There are several reasons why a company should leverage outsourced specialized SOC (Security Operations Centre) services:

- Provide access to a broader range of security expertise and resources than available in-house, including latest threat intelligence and cutting-edge security technologies.
- Outsourcing can prove cost-effective, as building an in-house SOC can be expensive and time-consuming.
- Tailored monitoring and incident response (including 24/7), which may not be feasible for an in-house team.
- Free up internal resources, allowing them to focus on core security program and strengthening their KPIs & KRAs.

Let's see how a central log management can help during an actual attack.



SIEM platforms render logs immutable and hence SIEM data and reports can be presented in a court of law as the chain of custody was maintained and data integrity retained.

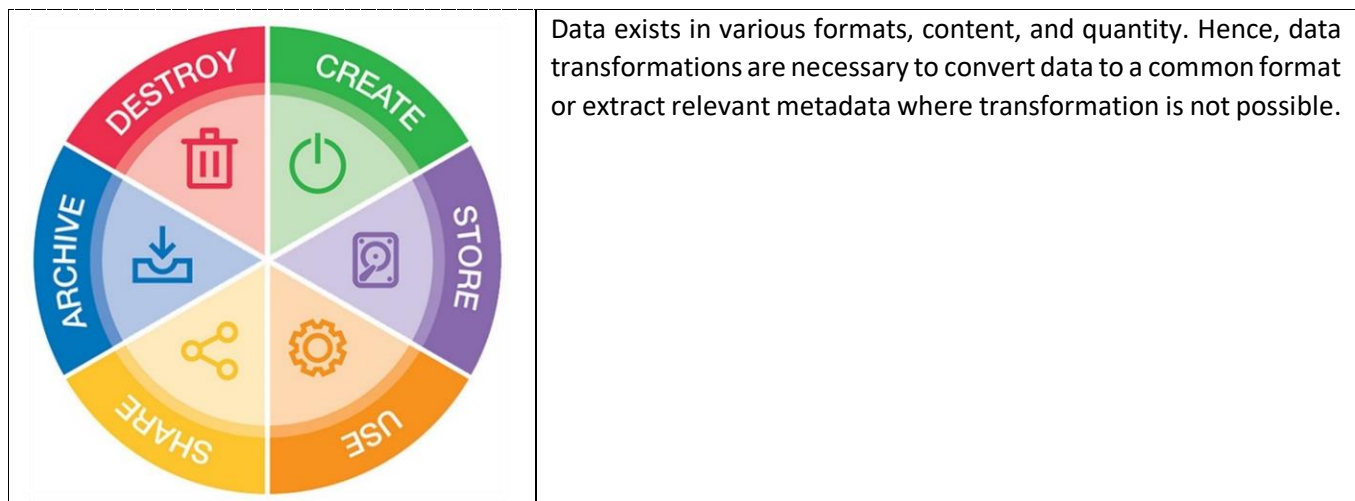
## Chapter 11: Data Lifecycle Management

You may have heard “Data is the new Oil”.

We’d say “Data is the new radioactive material”  
It’s harmful to hold a lot and hold it for long.

Data lifecycle management is the process of managing data from its creation to its eventual disposal. It is a critical component of any business, especially for startups, as it ensures data management and security. Startups should strive to securely collect **ONLY** necessary operational data and track it for security and privacy reasons.

Data collected is ultimately securely disposed of when no longer needed. It’s entirely possible that certain transactional data will be retained for years due to regulatory and compliance requirements.



[Read More: <https://www.clicdata.com/blog/complete-guide-data-lifecycle-management/>]

By following these best practices, startups can ensure that their data is properly managed and secured.

### 11.1 Data Collection

Ingesting or collecting data can come from different sources and varying formats (text, photo, audio, video) is an important part of data lifecycle management. Startups should strive to collect only the data that is necessary for their operations. Collecting too much data can lead to privacy and security risks, as well as unnecessary costs. Startups should also keep track of the data they collect and ensure that it is properly stored and secured.

### 11.2 Data Classification

This can be a chapter, but in a nutshell consider classifying data in broad categories such as “Confidential”, “Internal Use Only”, “Public”. Leverage the industry standard [Traffic Light Protocol \(TLP\)](#) and labels can vary (even {L1, L2, L3}, {red, blue, green}) but do classify data since applying stringent security controls to public data will needlessly increase cost and effort.

### 11.3 Data Security

Startups should put processes in place to securely collect data via authorized users. This includes encrypting data, using secure protocols, and limiting access to restricted users. Consider onboarding a Data Leakage Prevention (DLP) tool early on. With new age cloud first companies, data security is not limited to endpoints like desktop/laptop/mobile/server etc. The data security plan should also consider the cloud-to-cloud (e.g., corporate Google Drive to personal Dropbox) data leakage probability.

### 11.4 Data Disposal

Finally, startups should ensure that they have a plan in place for disposing data when it is no longer needed. This includes securely deleting data, archiving it, or transferring it to another system. This helps to ensure that data is not exposed to unauthorized access and that it is disposed of in a secure manner.

### 11.5 Code = Data

Organizational data is not restricted to emails, texts, images, spreadsheets etc. It encompasses customer data, employee data and even application code (as applicable) in development environments. You must have read reports in the news about application source code leakage. This occurs due to lax security controls deployed within development environments.

While it may be tempting to jump on the AI bandwagon and use all the shiny online tools to analyse, refactor, and fine-tune your code, beware: sending your code out into the digital abyss could be like shouting your secrets into a megaphone. You might be getting cool outcomes, but at what cost? Don't let your code become a leaky faucet of information.

## Conclusion

In today's digital age, information security is critical for startups of all sizes, industries, and stages. As startups rely more on technology to operate and serve customers, they must take proactive measures to secure their data, systems, and processes from potential security threats.

In this e-book, we have explored several key information security considerations that startups must address to effectively protect their sensitive information, including:

- **Cybersecurity Planning:** establish a cybersecurity plan that outlines the organization's goals, strategies, and tactics for protecting its sensitive information.
- **Information Security Policies:** develop and implement robust information security policies that establish how the organization will protect its data and systems.
- **Employee Training:** provide ongoing employee training to ensure that workers understand and follow appropriate security practices.
- **Vendor Management:** rigorously manage third-party vendors and contractors to ensure they follow appropriate security practices.
- **Incident Response Planning:** develop and implement a comprehensive incident response plan to ensure that they can respond quickly and efficiently to security incidents.
- **Data Backup:** 100% protection from ransomware is backup, backup, and backup.
- **Talk to Experts:** When in doubt or need expertise, don't shy from onboarding a vCISO.

By implementing these security measures, startups can effectively manage their security risks, protect their sensitive information, and build trust with their customers.

However, cybersecurity is an ever-evolving field, and startups must remain alert and adaptive to new security threats and vulnerabilities. We encourage startups to stay informed about emerging security trends and best practices, regularly assess their security posture, and continually improve their information security programs.

We hope this e-book has provided valuable insights and guidance on information security for startups. Remember, proactive information security is critical for building a successful and sustainable business in today's digital age.

In case you ever need any further assistance in planning and optimizing your data security practices, feel free to get in touch with us.

*"Cyber Security for Startups" is a must-read for any startup founder or entrepreneur wanting to protect their business and data from cyber threats. In this book, you'll discover information security best practices, tailored to your startup's stage of growth.*

*With insights into the Indian regulatory environment and practical guidance, this book offers a starting point you need to embark your security journey.*

***Don't let cyber threats derail your business.***

This e-book features valuable insights of experienced cyber security professionals who understand the importance of balancing security and usability, while making security management easy.



### **Rohit Srivastwa**

Serial entrepreneur and 20+ years of experience in information security, secure digital transformation, and incident response. Advises corporates, and government bodies of different countries.



@rohit11



/rohit11



<https://rohit11.com>



### **Aalok Karnik**

18+ years of experience in enterprise security. Managed various security projects at Fortune 100 companies like Google, McAfee, HP, Walmart, Twitter etc.



@aalok\_the\_k



/aalok